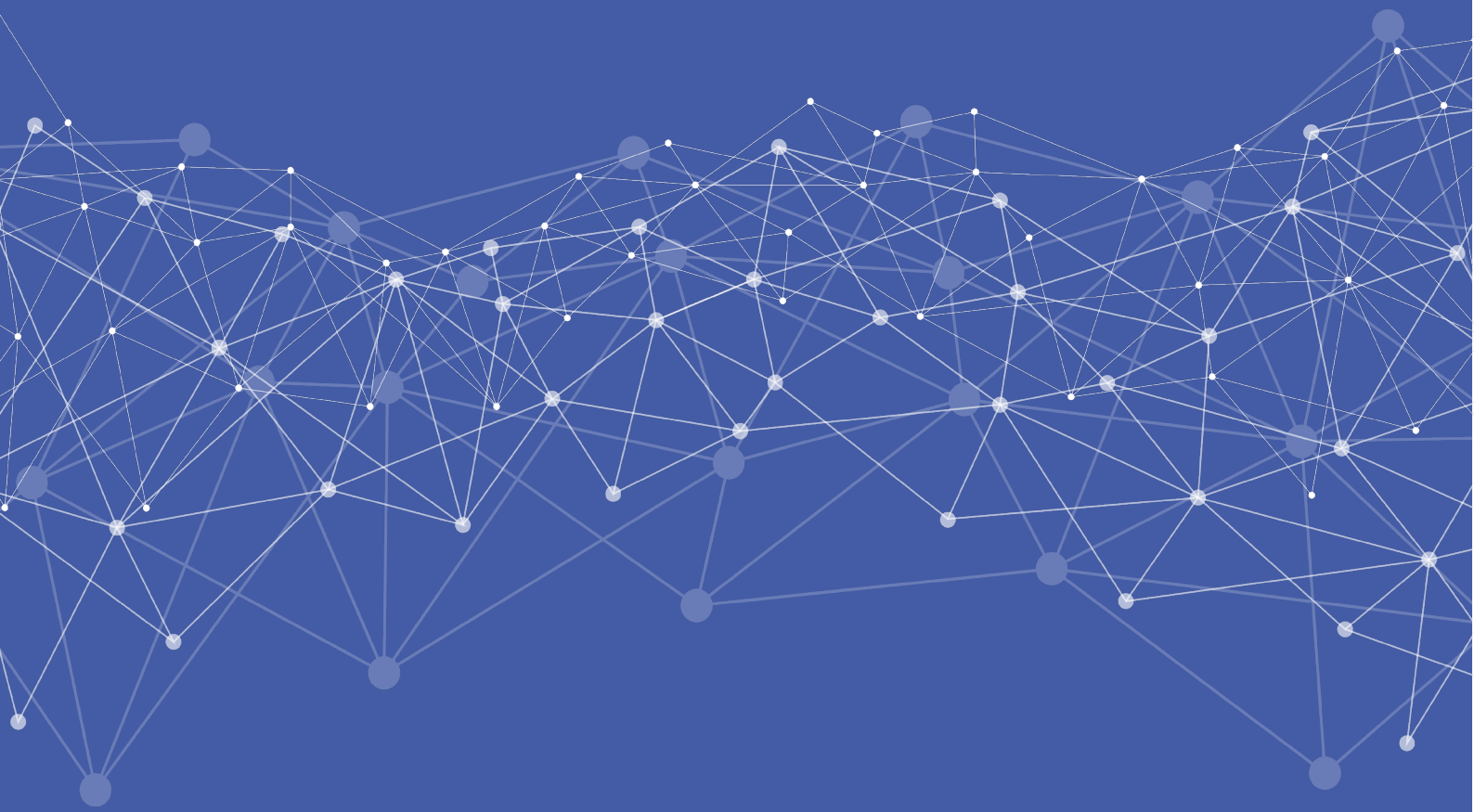
CYBERFORT



G-Cloud 14

Standard Terms & Conditions
Security Testing

Standard Terms & Conditions

The below Standard Terms and Conditions are applicable to the supply of the G-Cloud Framework and would form the Services to be supplied under the Call-Off Contract with the Customer/Buyer.

If you ultimately decide to purchase the Service(s) described with Cyberfort, then all terms and conditions will only be pursuant to a final and definitive written agreement between the Customer/Buyer and Cyberfort (including any amendments, if applicable).

For the avoidance of doubt, the final agreement will replace any other suggested terms and conditions.

Notwithstanding anything to the contrary, Cyberfort makes no representations, warranties, or covenants (including without limitation as to any products, services, service levels, third-party products or services or interoperability) separate from, in contravention of, or in addition to those contained in the final agreement, and any purported representation, warranty or covenant in this information document shall be of no force or effect.

Any information provided in below regarding the Service is for informational purposes only and is subject to change.

Security Testing

1. Definitions and Interpretation

The definitions shall apply to these Terms and Conditions unless otherwise stated.

Customer/Buyer	means the individual(s) and/or organisation(s) that is ordering the Services;
Cyberfort	means Cyberfort Limited;
Applicable Law	all applicable laws, statutes, regulation and codes from time to time in force;
Consultant	means the individual(s) provided by Cyberfort for the performance of the Security Testing;
Contract	together, these Standard Terms and Conditions, the Order Form and its Schedules, the Framework Agreement and any other documents referred to in them;
Cyberfort Materials	all software programs (including the Software), applications, documents, processes, methods, know-how and data, including any modifications, enhancements and developments thereto, owned by or licensed to Cyberfort and used in the provision of the Service;
Data	the digital information provided by Customer/Buyer to Cyberfort through the use of the Software to be stored on Cyberfort servers as part of the Services;
Order Form	means an order form agreed between the parties to request one or more of the Services;
Penetration Test Authorisation Form	means the form to be signed by the Customer/Buyer and submitted to Cyberfort when ordering the Security Testing;
Security Testing	means the process of testing the System as described in the Order Form;
Service	One or more of the Service(s) to be provided by Cyberfort to the Customer/Buyer pursuant to a Order Form;
Service Levels	the service levels applicable to each Service (if any) as set out in the Order Form;
System	means the systems and networks which the Customer/Buyer requires to be security tested pursuant to this Contract;
Test Report	means the report produced by Cyberfort detailing the results of the Security Testing;

2. Provision of the Testing Services

2.1 Cyberfort shall provide the Testing Services on the System in accordance with the terms of the Agreement.

2.2 The Customer confirms its consent, for itself and on behalf of all group companies to Cyberfort performing the Testing Services and confirms that it has procured, where necessary, the consent of all its (and its group companies) employees, agents and sub-contractors that Cyberfort shall be permitted to carry out the Testing Services. Cyberfort will be carrying out the Testing Services in the belief that it has all appropriate consents, permits and permissions from the Customer and its group companies (and their employees, agent and sub-contractors).

2.3 If the parties executed a Penetration Test Authorisation Form to enable Cyberfort to commence Testing Services prior to the date the Order Form was agreed, Penetration Test Authorisation Form shall be deemed to have been made under and pursuant to the terms of the Agreement.

3. Cyberfort obligations

3.1 Cyberfort shall provide:

a) the Service with reasonable care and skill and materially in accordance with the applicable Order Form, including, where applicable, the Service Levels; and

b) such cooperation and information reasonably requested by the Customer/Buyer in respect of the Service.

3.2 Where a Test Report is required it shall, unless otherwise agreed, be produced by the Consultant within twenty-eight (28) days of completion of the Testing Services and sent to the Customer.

3.3 Whilst Cyberfort will use all reasonable endeavours to ensure that the same Consultant will continue throughout the Testing Services, it reserves the right to replace that Consultant if necessary.

3.4 Cyberfort shall, where the Consultant is present on the Customer's premises, ensure that the Consultant complies with such reasonable site rules and procedures as are notified to Cyberfort from time to time.

4 Customer/Buyer obligations

4.1 The Customer/Buyer shall:

a) obtain appropriate consent from its ISP and any other relevant third-party supplier of the System for the Testing Services to be carried out and, when requested by Cyberfort, to provide evidence of such consent and to notify relevant employees that the Testing Services has been scheduled and that they may be monitored;

b) arrange a mutually convenient time with Cyberfort for the performance of the Testing Services and to inform its ISP of the date agreed with Cyberfort;

c) make appropriate backups of the System prior to the commencement of the Testing Services;

d) ensure that suitable accommodation and working conditions are provided for the Consultant which shall include network access and, where necessary, access to data centres, server rooms and/or switch rooms where the Testing Services is to take place on the Customer's premises;

e) provide all necessary hardware (e.g. mobile device or security token) for a security test by Cyberfort, and will deliver the hardware to the relevant Cyberfort premises and collect it from those premises or authorise other means of delivery and return at the Customer's own risk. Cyberfort shall not be liable for the hardware during transit to or from its offices;

f) provide Cyberfort with at least one employee who shall have substantial computer systems, network and project management experience of the Customer's Systems to act as liaison between the Customer and Cyberfort;

g) co-operate with Cyberfort and provide it promptly with such information about its Systems, network, premises, equipment, data structures, protocols, software, hardware and firmware as are reasonably required by Cyberfort;

h) ensure that, where the Testing Services is taking place on its premises, the premises is safe;

i) whilst Cyberfort will conduct all Testing Services in line with accepted best practice and make all reasonable efforts to avoid disruption of the Customer's network, the tools and techniques used may cause disruption to the Customer's Systems and/or possible loss of or corruption to data, and the Customer will take such backups and provide such redundant systems as are prudent in the circumstances;

j) notify Cyberfort if there are any periods during Testing Services when Cyberfort should stop work due to critical business processes (such as batch runs) or if any part of the System is business critical so that Cyberfort can, if needs be and with the Customer's consent, modify its testing approach; and

k) where Cyberfort supplies any software as part of the Testing Services, only use such software for lawful purposes.

SCHEDULE 1 – PENETRATION TEST AUTHORISATION FORM

1. Authorisation to perform Penetration Testing Services

Service Provider	Service Recipient
Cyberfort Limited Venture West Greenham Business Park Thatcham RG19 6HX	*[Insert Customer/Buyer details]*

1.1 This authorisation grants permission to Cyberfort to perform a penetration test against the systems as described in the section Target Systems during the period described in section Testing Timeframe.

2. Testing Timeframe

From	To
[Insert testing start date]	*[Insert testing finish date]*

3. Target Systems

Target Systems
[Insert IP addresses/ranges or URLs]

4. The Service Recipient warrants and acknowledges:

4.1 The system information provided above is owned by or operated on their behalf and that they have authority to approve security testing against these systems.

4.2 All parties that may be affected by the testing have been informed of the nature of the test.

4.3 While Cyberfort shall use reasonable care and skill in performing the test, Cyberfort cannot and does not warrant that no damage or loss of availability will be sustained by the target systems.

4.4 All employees who need to be aware of the testing, for legal or operational purposes have been notified.

4.5 Cyberfort does not offer any implied or express guarantees that the results of the tests will mean that the Customer/Buyer's network is secure from every form of attack, as Internet Security is continually growing and changing matter.

5. Cyberfort acknowledges that:

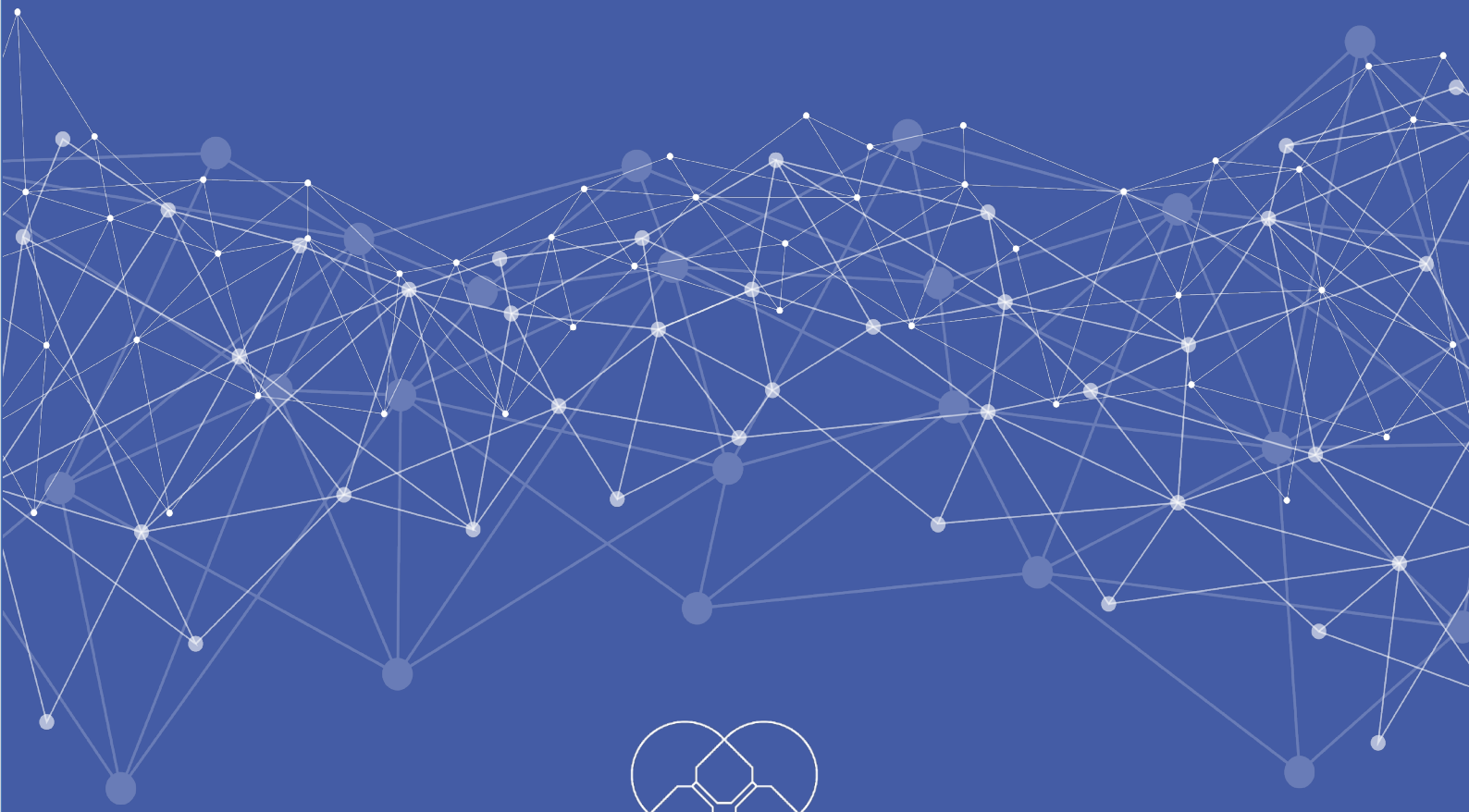
5.1 If an intruder is discovered on the Customer/Buyer's information system during the testing, the test will be suspended, and the incident reported to the Customer/Buyer.

5.2 At any time during the tests, the Customer/Buyer can request that Cyberfort stop testing.

5.3 During the engagement, the source IP addresses will be:

- [TBC]
- [TBC]

Please note that if you have an Intrusion Detection System (IDS) Cyberfort may generate a fair amount of noise from these addresses in your network logs.



CYBERFORT

www.cyberfortgroup.com

For more information, please contact us on:

01304 814800

info@cyberfortgroup.com